ASIGNATURA: LEGISLACION

APUNTES DE CATEDRA

TEMA: HABEAS DATA

ANTECEDENTES

El concepto de protección de datos nació como una mera contraposición a la interferencia en la vida privada de las personas facilitada por el avance tecnológico. Sin embargo, con el transcurso del tiempo, esa concepción fue evolucionando hasta llegar al momento actual en el que la doctrina internacional lo entiende como la protección jurídica de las personas en lo concerniente al tratamiento de sus datos personales, tanto en forma manual como automatizada. Por otro lado, también ha evolucionado la concepción del derecho a la vida privada, pues ha dejado de concebirse como la libertad negativa de rechazar u oponerse al uso de la información personal para convertirse en la libertad positiva de supervisar su uso.

En consecuencia, en la actualidad algunos definen el concepto de protección de datos como el amparo debido a los ciudadanos contra la posible utilización de sus datos personales por terceros, en forma no autorizada, para confeccionar una información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad o como la protección de los derechos fundamentales y libertades de los ciudadanos contra una singular forma de agresión: el almacenamiento de datos personales y su posterior cesión.

Más allá de la reconocida evolución doctrinal de este concepto, es indudable que con el correr de los años la posibilidad de disponer información sobre las personas ha ido paulatinamente en aumento. Si a ello se le suma el importante papel que las bases de datos desempeñan en el mundo tecnificado y globalizado de hoy, surge con pocos cuestionamientos el derecho de las personas a protegerse frente a la intromisión de los demás.

En definitiva, el bien jurídico subyacente es la autodeterminación informativa que consiste en el derecho que toda persona tiene a controlar la

información que le concierne, sea íntima o no, para preservar de este modo y en último extremo, la propia identidad, su dignidad y libertad. Este derecho a la autodeterminación informativa fue llamado por primera vez de esa manera en la sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983, que declaró inconstitucionales ciertos aspectos de la Ley del Censo de Población de 1982 de la República Federal Alemana.

La referida sentencia destacó como contenido del derecho a la personalidad la facultad de decidir por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida. Reconoció además que esta facultad requiere de especiales medidas de protección ya que la interconexión de varias colecciones de datos puede converger en la elaboración de un perfil de la personalidad y puede influir en la autodeterminación del individuo y en su libertad de decisión.

Resumiendo, basado en la exigencia de consentimiento para que la recogida y el tratamiento de datos sean lícitos, el derecho a la autodeterminación informativa sobre el que se apoya el concepto de protección de datos personales, no sólo entraña un específico instrumento de protección de los derechos del ciudadano, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona y decidir sobre la difusión y la utilización de sus datos personales.

Así lo ha entendido el Tribunal Constitucional Español, al decir que el derecho fundamental a la protección de datos persigue garantizar a las personas el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

INCORPORACION EN EL DERECHO ARGENTINO

La garantía del Hábeas Data fue incorporada por la reforma constitucional de 1994 en el tercer párrafo del artículo 43 de la Constitución Nacional, en estos términos:

"...Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de

datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, la rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".

Asimismo, la protección del derecho a la intimidad así consagrado en la Constitucion Nacional, se encuentra reglamentada por la ley 25.326, estableciendo una serie de reglas y principios para los archivos públicos y privados destinados a dar información.

Concepto

El Habeas Data podemos definirlo como aquella garantía en virtud de la cual toda persona tiene el derecho de solicitar por vía judicial, que le sean exhibidos los registros, tanto públicos como los privados destinados a dar informes, en los cuales obren sus datos personales o los de su grupo familiar, para poder tomar conocimiento de su exactitud y requerir en caso necesario su rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación. Esta herramienta tiende a proteger a la persona contra calificaciones erróneas, incompletas o sospechosas, incluidas en registros, que pueden a llegar a perjudicarle de cualquier modo.

EL BIEN JURÍDICO TUTELADO

Se trata de una garantía que protege fundamentalmente el derecho a la intimidad, sobre todo frente a los avances del llamado "poder informático", que en muchas ocasiones lesiona este derecho reconocido en el artículo 19 de la Constitución Nacional.

En la actualidad el derecho a la intimidad ya no puede reducirse a excluir a los terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal que de él figura en los registros, archivos y bancos de datos, sean estos públicos o privados.

Tal instituto protege un "complejo de derechos personalísimos", que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad. Lo que se pretende lograr es la autodeterminación informativa que consiste en el derecho que toda persona tiene

a controlar la información que le concierne, sea intimo o no, para preservar de este modo y en último extremo, la propia identidad, su dignidad y libertad.

Existen fundamentalmente dos bienes jurídicos a tutelar:

(a) el derecho a la exactitud de los datos inherentes a la persona que pudieren estar registrados en un archivo, registro o base de datos que no sean de exclusivo uso personal de su titular o administrador;

(b) el derecho a que permanezcan en la intimidad de la persona los datos considerados sensibles.

Nuestro más alto Tribunal de Justicia ha reafirmado la existencia de esta garantía constitucional diciendo que: “El creciente almacenamiento y recopilación de datos de carácter personal en el mundo moderno, facilitado en gran parte por el avance de la informática, torna razonable consagrar un derecho especial que proteja a las personas humanas para controlar la información que de ellas consta en los registros, archivos o bancos de datos.

En nuestro país, se ha utilizado el hábeas data en varios casos como simple medio de acceso a la información. Sin embargo, ello no implica negar que, además de acceder a la información, el hábeas data posee otra finalidad que es la de corregir información falsa o discriminatoria.

Así es que el Art. 43 divide el hábeas data claramente en dos etapas: la primera, relativa al acceso a la información, y la segunda, después de comprobada la falsedad o la discriminación, destinada a corregir, rectificar, suprimir o someter a secreto el dato.

Lo que preocupa a los individuos además del almacenamiento de sus datos personales, y del riesgo que se incluyan datos de carácter sensible en los ficheros automatizados o no, es la posibilidad de controlar la veracidad de la información y el uso que de ella se hace.

Datos personales: “Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”. Esta definición legal parecería excluir, en principio, a aquella información que provenga de investigaciones epidemiológicas o que involucren determinadas poblaciones, ya que se trata de información colectiva y no referida a personas físicas o jurídicas

determinadas o determinables. Ello es así ya que la propia ley en el artículo 28° plantea la exclusión de “las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable”. Sin embargo puede tratarse de información “sensible”, como acontece por ejemplo, en el estudio de la prevalencia de enfermedades endémicas o características étnicas de una comunidad determinada, en la predisposición genética de grupos en riesgo de adquirir determinadas dolencias. Estos “datos sensibles comunitarios”, deben ser objeto de cuidado y protección; a pesar de no estar expresamente incorporados en la Ley de Proteccion de Datos Personales, existen normas, aceptadas internacionalmente, que prevén y regulan ese tipo de investigaciones.

Datos sensibles: “Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.” Las muestras biológicas, en especial, aquellas que contienen información sobre el código genético personal, deberían quedar incluidas en esta categoría; en especial por el particular auge que los estudios de Farmacogenética están teniendo en la actualidad. La referencia a la salud como dato sensible, debe incluir, además, toda aquella información que, aunque “stricto sensu” no se encuentre relacionada directamente con la misma, se haya recolectado con fines asistenciales o de investigación, como por ejemplo hábitos de vida, de consumo, historia personal y antecedentes familiares, etc.

Archivo, registro, base o banco de datos: “Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso”. En esta categoría se incluyen historias clínicas, fichas de atención ambulatoria, partes quirúrgicos y/o anestésicos, legajos médicos de servicios de medicina laboral, resultados de estudios clínicos y de laboratorio (en este caso debe prestarse especial cuidado a los registros de serologías para determinar la presencia directa o indirecta del

virus VIH, ya que existe normativa especial para proteger la intimidad en estos supuestos) En el ámbito de la investigación clínica todos los documentos que recolecten información sensible de cada sujeto de investigación deben incluirse en esta categoría: Legajo de seguimiento individual (Case Report Form CRF), registro de eventos adversos (SAE), archivos de los comités de revisión institucional (Institutional Review Board IRB) o comités de ética independiente, entre otros.

Tratamiento de datos: "Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias".

Responsable de archivo, registro, base o banco de datos: "Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos."

Datos informatizados: "Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado."

Titular de los datos: "Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley."

Usuario de datos: "Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos."

Disociación de datos: "Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable."

En el sistema de protección de datos sensibles y personales existen distintos mecanismos particulares para hacer efectiva la tutela de la información; en ese sentido se han distinguido y definido distintas versiones de la garantía del hábeas data.

HÁBEAS DATA PROPIO

El hábeas data en sentido estricto corresponde a toda acción destinada a incidir directamente sobre los datos sensibles y personales obrantes de registros. En esta versión existen dos tipos, **el hábeas data informativo**, vinculado al acceso y conocimiento del tipo de dato, ubicación del registro, finalidad del registro, fuentes de obtención; tiene características preventivas ya que se trata de conocer cuál es la situación para poder luego ejercer acciones concretas de supresión y/o rectificación.

El segundo tipo es el **hábeas data reparador**, que a su vez presenta una variada gama de subtipos y subespecies, en este caso se trata de producir modificaciones como mecanismo de protección efectiva a los derechos involucrados. En este último caso la petición modificatoria puede consistir en el aditamento, actualización o aclaración de la información. Del mismo modo puede acontecer que se requiera la corrección de datos falsos, inexactos o imprecisos. También puede solicitarse la eliminación total o parcial de los datos registrados, cuando por ejemplo la colecta y almacenamiento no se condicen con la finalidad del banco o base de datos.

En algunos casos especiales la acción sobre el banco de datos puede consistir en la solicitud expresa en que se mantenga o refuerce el sistema de protección de la intimidad y confidencialidad; mientras que en otros, cuando el dato deba estar anonimizado, podrá interponerse la acción de hábeas data a los efectos de solicitar la disociación irreversible entre la información y su titular.

Archivos, Registros o Bases de Datos privados destinados a proveer informes

Existen numerosos archivos, registros o bancos de datos privados que no tienen como finalidad principal suministrar informes a terceros, pero que recolectan información personal que puede resultar inexacta y/o discriminatoria en perjuicio de sus titulares.

No puede admitirse que los derechos de las personas sean vulnerados por el solo hecho de estar sus datos personales registrados en un archivo, registro o banco de datos que no está destinado a dar informes.

El Art. 24 de la ley 25326 dispone que deberán inscribirse en el registro del Art. 21 los archivos, registros o bancos de datos que no sean para un uso exclusivamente personal, sin distinguir entre aquellos que estén destinados a proveer informes o no. Ello da lugar a una interpretación amplia acerca de cuales son las entidades privadas enmarcadas en la Ley, criterio que es el seguido por otras legislaciones, en el cual se excluye de las normas de protección sólo a los registros o archivos de uso personal o doméstico.

Al respecto cabe hacer notar que hay archivos internos que no están destinados a proveer informes a terceros, pero que exceden el uso personal de quien los administra, porque con ellos se realizan todo tipo de análisis que habrán de tener una incidencia, sin duda muy relevante, en los derechos del titular de los datos. Podemos citar como ejemplo, los legajos de personal, en los cuales se registra información objetiva que puede ser cuestionada por inexacta, o bien, se utilizan para registrar otro tipo de información que puede ser discriminatoria o bien agraviante. Lo mismo ocurre con las historias clínicas.

El Poder Ejecutivo. establece en el Art. 1° del decreto 1558/2001 que quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

PRINCIPIOS FUNDAMENTALES DE LA PROTECCIÓN DE DATOS.

Los principios generales de la protección de datos son los que definen las pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados en los archivos, registros, bancos o bases de datos, cuanto la congruencia y la racionalidad de la utilización de los mismos.

Contenidos fundamentalmente en el Capítulo II de la ley, pero rectores de todo su articulado, pueden reducirse a los siguientes:

a) Principio de pertinencia.

El primer principio que ha inspirado la Ley es el principio de pertinencia de los datos.

También conocido como principio de proporcionalidad y calidad de los datos, este principio exige que los datos que se recaben y almacenen en una base de datos sean pertinentes y adecuados, es decir, que estén relacionados con el fin perseguido en el momento de creación de la base de datos.

En una palabra, significa que la recolección y el tratamiento de los datos han de ser proporcionales con respecto a los fines que se persiguen, sin que en ningún caso se puedan utilizar los datos obtenidos para finalidades distintas de aquéllas para las que se hubieran recogido.

Así lo impone el artículo 4, inciso 1 referido a la calidad de los datos diciendo que los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

El principio de pertinencia, por tanto, delimita las circunstancias personales sobre las que pueden indagar y recabar información quienes mantengan bases de datos que incluyan información personal.

De tal forma, este principio supone que no obstante la posible autorización del titular de los datos o la habilitación legal para someter la información a tratamiento, no se permite que puedan incluirse más datos que aquellos que sirvan o puedan servir para la consecución de la finalidad que justifica dicho tratamiento, que debió determinarse en el momento de la obtención del consentimiento, o que sirve para presumir la concurrencia de éste en los supuestos en que se establecen presunciones legales de su otorgamiento.

b) Principio de finalidad.

Este principio, implica que los datos de carácter personal que sean recabados para incorporarse a una base de datos deben tratarse con un objetivo específico que debe conocerse antes de la creación de la base misma e informarse en el momento en el que la información personal es recolectada.

Varios artículos se refieren a este principio, siendo los más importantes el artículo 3, segundo párrafo que establece que los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública y el artículo 6, apartado a) que indica que cuando se recaben datos personales se deberá informar

previamente a sus titulares en forma expresa y clara la finalidad para la que serán tratados.

El principio de finalidad exige que los datos se obtengan y traten de manera leal y lícita, y que su almacenamiento se realice para unos fines concretos y legítimos.

c) Principio de utilización no abusiva.

El articulo 4, inciso 3 incorpora este principio diciendo que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

d) Principio de exactitud.

Los incisos 4 y 5 del artículo 4 establecen que los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario y que los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

De acuerdo al artículo 4 de la Ley los titulares de ficheros deben poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar su puesta al día. Este principio alcanza también a los supuestos de cesión. En estos casos el cedente debe notificar la rectificación o cancelación al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato (artículo 16, inciso 4).

Al exigir que los datos personales recogidos a los efectos de su tratamiento sean exactos y estén actualizados, con la correlativa obligación para el responsable del archivo, registro, banco o base de datos de suprimir, sustituir o completar aquellos datos total o parcialmente inexactos o incompletos, cabe entender también que será necesario proceder a su actualización conforme lo establecido por el artículo 16, pues aun cuando la ley sólo alude al deber de suprimir, sustituir o completar la información de que se trate, y no al deber de actualizar, este último debe entenderse implícito ya que una información que no esté al día puede ser considerada inexacta o incompleta. Este criterio ha sido el

adoptado en el primer párrafo del artículo 16 del Decreto 1558/2001 al aclarar que en las disposiciones de los artículos 16 a 22 y 28 a 43 de la Ley en que se menciona a algunos de los derechos de rectificación, actualización, supresión y confidencialidad, debe entenderse que tales normas se refieren a todos ellos.

Parece lógica la necesidad que los datos que se obtengan y se sometan a procesamiento sean exactos y estén actualizados. Cuando la información la aporte el titular de los datos se entiende que será completa y actualizada. Pero si los datos se obtienen por otros medios puede ocurrir que la información esté desactualizada, no se corresponda con la realidad o sea errónea, circunstancias que menoscabarán el legítimo interés de su titular. Por ello, el cumplimiento de la exigencia de que los datos sean exactos y actualizados recae sobre los responsables de los archivos o bancos de datos, siendo ellos los obligados por la ley a cumplir con el principio de exactitud. En definitiva, lo que pretende este principio es que los datos respondan con veracidad a la situación real de su titular.

e) Principio de derecho al olvido.

Intimamente relacionado con el principio de exactitud se encuentra este principio, también conocido como principio de limitación en el tiempo, que implica que los datos deben desaparecer del archivo o base de datos una vez que se haya cumplido el fin para el que fueron recabados. El inciso 7 del artículo 4º de la ley recepta este principio estableciendo que los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. Refuerza este principio lo establecido por el párrafo tercero del artículo 4 del Decreto 1558/2001 que al reglamentar su ejercicio indica que “el dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos”.

f) Principio de legalidad.

También conocido como principio de limitación de la recolección , establece que el procedimiento de recogida de datos no debe ser realizado en forma ilícita o desleal. Así lo establece el artículo 4, inciso 2 diciendo que la recolección de datos

no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.

Además de los que la ley contempla expresamente, a modo de ejemplo, pueden mencionarse como métodos fraudulentos, ilegales o desleales de recolección de datos a las investigaciones privadas realizadas por detectives, el uso de instrumentos de grabación o escucha de conversaciones privadas, la violación de correspondencia o papeles privados, o cualquier otro en el que se oculte la verdadera finalidad de la recogida de datos y posterior tratamiento. Lo que pretende la ley es evitar actuaciones delictivas por intermedio de las cuales pueda vulnerarse el bien jurídico protegido.

La ausencia de mayor precisión al respecto, motivó que se incorporara en el primer párrafo del artículo 4 del Decreto 1558/2001 una mención a los parámetros generales que deberan tenerse en cuenta para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne. En consecuencia, los parámetros que deberán analizarse serán el procedimiento efectuado para la recolección de los datos y, en particular, el cumplimiento de lo dispuesto por el artículo 6 de la ley en cuanto a la información que debe proporcionarse a las personas cuando se pretenda recabar información de carácter personal referida a ellas.

g) Principio de publicidad.

El artículo 21 establece que todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite la Dirección Nacional de Protección de Datos Personales. Ello porque tal como lo indica el artículo 3, la formación de archivos de datos será lícita cuando los mismos se encuentren debidamente inscriptos, observando en su operación los principios que establece la ley y las reglamentaciones que se dicten en su consecuencia.

La conveniencia de la creación y mantenimiento de un registro público en el que figuren los archivos o bases de datos que poseen datos de carácter personal, radica en que a través de su consulta los ciudadanos pueden tomar conocimiento de los archivos en los cuales pueden existir datos referidos a su persona y de la

identidad de los responsables de su tratamiento, para poder ejercer una defensa adecuada de sus derechos.

h) Principio de control.

Este principio, que la ley comentada incorpora en su artículo 29, se refiere a la existencia de un organismo de control responsable del cumplimiento efectivo de los principios contenidos en la legislación.

Todas las legislaciones del mundo que amparan los datos personales, tanto nacionales como supranacionales, han previsto un organismo de tales características. Sin embargo, no todas han estado de acuerdo en la forma adoptada para ello. Algunas han buscado la total independencia del Poder Ejecutivo, mientras que otras lo configuraron como un apéndice más del mismo.

En Argentina, algunos proyectos pretendieron ubicarlo en el ámbito del Congreso de la Nación creando una Comisión Bicameral de Protección Legislativa de Datos, otros propusieron la creación de una Comisión Nacional de Datos Personales integrada por miembros provenientes de distintos sectores de los poderes legislativo, ejecutivo y judicial, algunos bregaron por su independencia y otros lo subordinaron al Poder Judicial.

La versión original sancionada por el Congreso había optado por una opción intermedia. Dotaba al órgano de control de autonomía funcional, pero lo reconocía como un órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación, cuyo Director debía ser nombrado por el Poder Ejecutivo con acuerdo del Senado y podía ser removido por el Poder Ejecutivo por mal desempeño en sus funciones.

Aunque podía vislumbrarse su dependencia del Poder Ejecutivo, que se encuentra autorizado a determinar sus características organizativas por el artículo 45, con el veto parcial del Decreto 995 anteriormente mencionado se abrió una incógnita con relación al carácter autónomo, independiente o subordinado que ostentaría el organismo de control a crearse.

Como ya hemos visto, dicha incógnita fue dilucidada por el artículo 29 del Decreto 1558/2001, cuyo inciso 1 creó como órgano de control a la Dirección Nacional de Protección de Datos Personales.

Si bien es cierto que el sistema establecido por la ley carecería de eficacia si no se instrumentara un adecuado mecanismo de control sostenido por un organismo de tipo institucional, la condición básica para que su desempeño sea eficaz es que cuente con la independencia y potestades necesarias para poder supervisar, sin condicionamientos, que los responsables y usuarios de los archivos, registros, bancos o bases de datos públicos y privados sometan el tratamiento de los datos de carácter personal en ellos asentados a las disposiciones de la ley. Su creación dentro del ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos no augura tal independencia.

i) Principio de seguridad.

Una de las cuestiones que más preocupan en el tratamiento de datos en general, y de los datos personales en particular, es el de su seguridad, tanto en el momento de su recolección como en el de su tratamiento y cesión a terceros. Es por ello que el inciso 2 del artículo 9 prohíbe que se registren datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Entiendo que una de las misiones del Decreto reglamentario era establecer los niveles de seguridad que deberán adoptarse en cada caso concreto. Sin embargo, en su artículo 9, el Decreto 1558/2001 evita fijar estándares de seguridad indicando que será la Dirección Nacional de Protección de Datos Personales por él creada quien deberá “promover la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización”.

j) Principio de defensa de los datos sensibles.

A poco que se analizan las definiciones que la ley trae en su artículo 2º se comprende que no todos los datos personales requieren de idéntica intensidad protectora, pues la primer definición se refiere a los datos personales y la segunda a los datos sensibles, diferenciados de los primeros. Asimismo, a medida que se

avanza en el análisis de la ley aparecen diversas normas que se refieren de manera especial a cada tipo de datos.

La ley entiende por datos personales a cualquier tipo de información referida a personas físicas o de existencia ideal determinadas o determinables. Por su parte considera datos sensibles a aquellos datos personales que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
Como regla general, de acuerdo a lo establecido por el artículo 7, inciso 3, está prohibido formar de archivos, bancos o registros que almacenen información que directa o indirectamente revele este tipo de datos. Sin embargo, entiendo que por ser la intimidad un derecho renunciable, nada impide el tratamiento de datos personales, aún de los denominados sensibles, cuando sean recabados con el consentimiento del titular de los mismos, siempre que se respeten los principios generales de la ley. Es por ello que en el inciso 1 del artículo 7 se pone de manifiesto que ninguna persona puede ser obligada a proporcionar datos sensibles. Sin que el titular de los datos sea obligado a comunicarlos y siempre que la información se obtenga con su consentimiento libre, expreso, informado y por escrito, considero que no existe impedimento para incluir en una base de datos información sensible de una persona, siempre y cuando se respeten todos los principios generales contemplados por la ley.

Vemos entonces que el principio general que prohíbe el tratamiento de este tipo de datos admite varias excepciones. Una de carácter general como la del consentimiento anteriormente mencionada, y otras, más específicas, como las mencionadas por el artículo 8 y por los incisos 2, 3 y 4 del artículo 7, contempladas expresamente en la ley.

En efecto, el artículo 8 permite que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud recolecten y sometan a tratamiento datos personales relativos a la salud física o mental de sus pacientes actuales o pasados, estableciendo la obligación de respetar los principios del secreto profesional.

Asimismo, los mencionados incisos del artículo 7 prevén distintas excepciones. El inciso 2 indica que pueden recolectarse y tratarse datos sensibles cuando medien razones de interés general autorizadas por ley, permitiéndolo además cuando la finalidad de la recolección y tratamiento sea estadística o científica y no puedan ser identificados sus titulares. El inciso 3, en su parte final, permite que la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales lleven un registro de sus miembros aunque ello implique el registro de datos sensibles. Por su parte, el inciso 4 establece que los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

k) Principio del consentimiento.

Como regla general, el tratamiento de datos de carácter personal requiere el consentimiento libre, expreso e informado del titular de los datos. El propósito del consentimiento requerido es el de proporcionar a la persona el derecho a elegir qué datos referidos a su persona pueden ser sujetos a tratamiento. El artículo 5 del Decreto 1558/2001 entiende en su primer párrafo que el consentimiento informado es aquél que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a la que se refiere el artículo 6 de la Ley.

En principio, el consentimiento debe constar por escrito. Si bien el artículo 5 de la Ley también permite que sea prestado por otro medio equiparable, el inciso 2 del Decreto 1558/2001 establece que será el órgano de control quien establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto al escrito.

Resulta importante destacar que una vez prestado el consentimiento, el titular de los datos puede revocarlo en cualquier momento, sin que se le puedan atribuir efectos retroactivos.

El inciso 2º del artículo 5º de la Ley enumera las excepciones al requerido consentimiento del titular de los datos para el tratamiento de sus datos personales. Los supuestos son los siguientes:

1) Cuando los datos se obtengan de fuentes de acceso público irrestricto;
2) Cuando se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
3) Cuando se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
4) Cuando deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
5) Cuando se trate de las operaciones que realicen las entidades financieras (29) y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la ley 21.526 (30).

La exigencia del consentimiento previo también sufre excepciones en el caso de cesión a terceros. En efecto, además de las excepciones previstas en general por el inciso 2º del artículo 5º, el inciso 3 del artículo 11 establece que no debe exigirse el consentimiento cuando:
1) Así lo disponga una ley;
2) La cesión se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;
3) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.
4) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables. A tal fin, y de acuerdo a lo que establece el párrafo cuarto del artículo 11 del Decreto 1558/2001, la Dirección Nacional de Protección de Datos Personales deberá fijar los estándares de seguridad aplicables a los mecanismos de disociación de datos.

Conclusión

El Habeas Data garantiza a las personas el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y

lesivo para la dignidad y derecho del afectado, y en su caso, posibilita la petición de que se suprima, rectifique o actualicen los datos.

Bajo este marco conceptual, los archivos de uso interno, si exceden el uso personal de quien los crea o administra, porque su contenido sirve para realizar evaluaciones que pueden tener una incidencia relevante en los derechos del titular de los datos, se encontrarán sujetos al contralor del titular de los datos allí asentados.

BIBLIOGRAFIA :

Gustavo Daniel Tanús. **"**Proteccion de datos personales. Principios generales, derechos, deberes y obligaciones" Artículo publicado en Revista Jurídica El Derecho. 19/06/2002, pág. 6. Buenos Aires, Argentina.

La Legislatura de Jujuy, Sanciona con fuerza de LEY Nº 5188

“REGULACION DE LA ACCION DE HABEAS DATA”

ARTICULO 1.- La acción tendiente a hacer efectiva la garantía prevista en los Artículos 43 tercer párrafo de la Constitución de la Nación Argentina y 23 apartados 6 y 8 de la Constitución de la Provincia de Jujuy se ejercerá conforme a las disposiciones de la presente Ley.-

ARTICULO 2.- Podrá deducir la acción de habeas data toda persona física o jurídica que acredite tener un interés legitimo, incluyendo los herederos hasta el cuarto grado de consaguinidad y el cónyuge, siempre que no estuviere divorciado; de la persona cuyos derechos resulten afectados.-

ARTICULO 3.- La acción de habeas data se deducirá en contra de cualquier persona publica o privada que tenga bajo su administración o custodia el registro, archivo o banco de datos, cualquiera sea su finalidad.-

ARTICULO 4.- Será competente para conocer en la acción de habeas data la Sala en turno de la Cámara en lo Civil y Comercial del lugar donde se encuentre ubicado el respectivo registro, archivo o banco de datos o del domicilio del actor, a elección de este.-

ARTICULO 5.- Previo a interponer la acción de habeas data, el peticionante deberá notificar fehacientemente su pretención al titular del registro, archivo o banco de datos. Solo ante la negativa o silencio del requerido quedara expedita la acción judicial. Se entenderá que existe silencio si la requisitoria no es contestada en el plazo de diez (10) días hábiles de recibido el requerimiento.-

ARTICULO 6.- El titular de la acción podrá ser asistido por asesores técnicos o jurídicos en el momento de tomar vista de los registros, archivos o bancos de datos que se le deban exhibir. También podrá requerir que a su costa se le expida copia certificada de la información allí contenida.-

ARTICULO 7.- La demanda deberá interponerse por escrito y contendrá:

a) El nombre y apellido, documento de identidad, domicilio real y constituido del demandante;

b) La individualización del archivo, registro o banco de datos sobre el que se quiere pedir informe o, en su caso, la institución o persona a cuyo cargo se encuentra. En caso de ignorarse esta circunstancia podrá solicitarse su identificación por orden judicial;

c) La relación circunstanciada de los datos que presuntivamente contendría dicho registro, archivo o banco de datos y los elementos que permitan apreciar el interés legitimo en la promoción de la acción respectiva;

d) El requerimiento, en términos claros y precisos, de la medida a tomar sobre esos datos, sise conocieran previamente, sin perjuicio del derecho de ampliar dicha petición con posterioridad al informe que se obtenga del demandado;

e) Juntamente con la demandada deberá acompañar la prueba documental que obrare en poder del actor y ofrecerse la restante.-

ARTICULO 8.- Luego de presentada la demanda y en cualquier estado del proceso, el Juez, a petición de parte, podrá decretar las medidas cautelares que entienda pertinentes, según las circunstancias del caso, a efectos de garantizar el resultado del proceso.

ARTICULO 9.- Admitida la demanda, el Juez requerirá al demandado la presentación de un informe en el que conste:

a) Si existe el registro, archivo o banco de datos denunciado;

b) Cual es el objeto y finalidad del mismo;

c) Todos los datos que tenga del actor;

d) Si se han requerido o emitido datos del mismo y en su caso a quien;

El Juez fijara el plazo dentro del cual debe producirse el informe, pudiendo, además, ampliar o restringir la información a requerir, según las circunstancias del caso.

Asimismo, el Juez podrá disponer todo tipo de medidas tendientes a compeler al demandado a producir el informe respectivo.

ARTICULO 10.- Producido el informe, el mismo será puesto a disposición del actor por el plazo de cinco (5) días a fin de que amplíe la demanda con relación a los datos informados y de ella se dará traslado al demandado, también por el

plazo de cinco(5) días, para que la conteste acompañando la prueba documental y ofreciendo las demás pruebas de que intente valerse.

ARTICULO 11.- Si la cuestión no resultare de puro derecho, el Juez abrirá la causa a prueba, estableciendo el termino para su producción.

ARTICULO 12.- Producida la prueba, sin necesidad de alegatos, el Tribunal dictara la sentencia dentro del plazo de diez(10) días.

si la sentencia admitiere la demandada, en ella se dispondrá:

a) La expresión concreta del particular o de la autoridad publica a quien se dirija y con respecto a cuyos registros, archivos o banco de datos se ha concedido la acción:

b) La determinación precisa de lo que debe o no hacerse;

c) El plazo para su cumplimiento que no podrá exceder de cinco (5) días.

ARTICULO 13.- La sentencia dejara subsistente el ejercicio de la demás acciones que pudieran corresponder con independencia de la acción de habeas data.

ARTICULO 14.- En todo lo no previsto son de aplicación supletoria las disposiciones de la Ley 4442 “Régimen Procesal para Amparo de los Derechos o Garantías Constitucionales que Carezcan de Reglamentación para su Tutela” y sus modificatorias y del Código Procesal en lo Civil y Comercial de la Provincia, en especial las que regulan el tramite del proceso sumarísimo.

ARTICULO 15.- Comuníquese al Poder Ejecutivo Provincial.

SALA DE SESIONES, San Salvador de Jujuy, 3 de Agosto de 2.000.-.

.